OIT-0999-88

20 OCT 1988

MEMORANDUM FOR: Chief, Intelligence Control Group
DO Policy and Coordination Staff

FROM: Edward J. Maloney
Director of Information Technology

SUBJECT: Proposal for a DCID Governing the Creation of
25X1 Computerized Data Bases [redacted]

REFERENCE: Your Memo, dtd 2 September 1988, Same Subject

1. The Office of Information Technology welcomes the opportunity to
25X1 participate in this working group. I have asked [redacted] Chief of
the Technical Security Division, to represent the office in the working
25X1 group. He may be reached at [redacted]

2. The task you are proposing is not an easy one to resolve, but it is an important one. The need-to-know principle is a double-edged sword; on one side it protects information against compromise or misuse; on the other side it enables or empowers the user or analyst. Clearly, computer technology and data bases have enhanced this latter capability from which the Intelligence
25X1 Community and the U.S. Government have benefitted greatly. [redacted]

3. The development of Intelligence Community policies for the accreditation of computer data bases will increase the control over Directorate of Operations' information. The challenge will be to arrive at policy which will result in protection of sources and methods, but which will
25X1 also further the enabling facet of the need-to-know principle. [redacted]

25X1 [redacted]

Edward J. Maloney

25X1 [redacted] [redacted]

25X1 SUBJECT: Proposal for a DCID Governing the Creation of Computerized Data Bases

25X1 C/TSD/MSG (17 Oct 88)

Distribution:
Original - Addressee w/att
2 - D/OIT w/att
2 - TSD/OIT w/att
1 - C/MSG/OIT w/att
3 - ISC/OIT wo/att

0922X88

SECRET

2 September 1988

MEMORANDUM FOR: See Distribution

25X1 FROM: [redacted]
Chief, Intelligence Control Group
DO Policy and Coordination Staff

SUBJECT: Proposal for a DCID Governing the Creation of Computerized Data Bases

1. Your participation is requested in a working group for the purpose of developing criteria for a new Director of Central Intelligence Directive (DCID) which would govern the creation of computerized data bases and the need to involve not only the accrediting authorities for these bases in U.S. Departments and Agencies but the data owners whose concurrence must be obtained before a computerized data base is established.

2. We are no closer today than we were five years ago when the undersigned first proposed the development of an intelligence community-wide computer security policy which would set forth standards for the accreditation of computer data bases and adherence to the compartmentation and need-to-know principles as defined in DCID 1/7. Without such a policy it is now impossible to ensure access to data banks by only those with a genuine need-to-know and to prevent use of computers for further dissemination of information to those not on the original dissemination of reports.

3. Thus far data owners have had little or no participation in the accreditation process for computer data bases to ensure that appropriate access controls are instituted in conformity with the need-to-know principle. There is no one place in the U.S. Government that could provide a listing of existing computer data bases and what types of information are included therein. Efforts in the past to obtain such a list through the intelligence community staff have been unproductive. There is no existing directive which obliges anyone to obtain the concurrence of data owners before a data base is created. The recent revision of DCID 1/16 is the first directive which requires concurrence by data owners. However, this applies only when actual or potential foreign national access may be involved in the design and implementation of a data base.

4. In this era of heightened counterintelligence concern, the Deputy Director for Operations has expressed his desire to bring the general availability of disseminated DO reports under better control, limiting access to this product to users who have a validated need-to-know.

25X1 [redacted]
25X1 [redacted]

SECRET

With the exception of "exclusive for" disseminations all electronically-disseminated DO reports are potentially available to any analyst with access to a data base.

5. There are some specific data bases (e.g., DESIST) in which DO representatives have participated in the development of data base management procedures and access controls. These bases have used the initial dissemination criteria or code as a means of defining need-to-know in retrospective retrieval of DO intelligence information reports. We still believe that this is the only viable alternative if we are to better control further use and dissemination of DO reports.

6. The general practice today followed by our electrical recipients is that if an individual is approved for the very sensitive "access control" codeword information it must be acceptable that he have access to the entire range of topics contained in a data base. Analysts make up their own profiles of what they need and by use of key words can obtain whatever else they want to see. We continue to argue that there must be a further demonstrated "need-to-know" before access can be permitted. Some data base managers continue to express the view that we are living in a benign environment and that we must have faith and trust in the analysts to delimit his or her access to only the specific assigned geographic or topical interests. This may be an admirable view; however, from a counterintelligence standpoint it is not realistic.

7. It is therefore strongly recommended that a new DCID be developed to govern the creating of and access to a data base with the full participation of data owners to ensure that full protection is afforded to their information consistent with well defined security standards to protect sources and methods.

8. The new DCID must also address the need for a records management policy for data bases so that specific periods of time are designated for the retention of reports and for the periodic purging of the data bases. This is vital in order to establish the extent of damage to sources and methods in the event of a hostile penetration of the data base.

9. Please advise the undersigned of your willingness to participate in this working group. Any observations or comments which you may have on the proposal and composition of the working group would also be appreciated.

25X1

SECRET

SUBJECT: Proposal for a DCID Governing the Creation of Computerized Data Bases

25X1

ADDRESSEES: [redacted]
Executive Staff,
formation Resources
ief, Intelligence Support Staff, CPAS
Special Assistant to ADDO/CI
, Acting Chief,
sment Branch, OS
ief, Information Security Staff, IMS
Special Assistant to EXDIR
O/DDO
O/DDI
O/DDA
O/EXDIR

SECRET